

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-184756

(43)Date of publication of application : 09.07.1999

(51)Int.Cl.

G06F 12/14

(21)Application number : 09-357756

(71)Applicant : TOSHIBA CORP

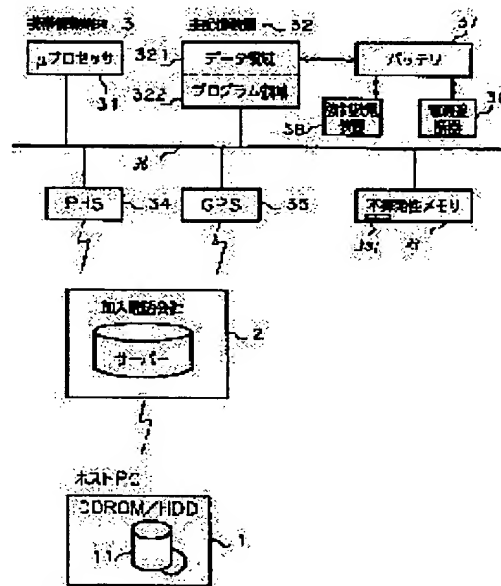
(22)Date of filing : 25.12.1997

(72)Inventor : NOSE MASAKI
NUMAJIRI YUTAKA**(54) SECURITY CONTROL METHOD IN PORTABLE INFORMATION TERMINAL AND SYSTEM THEREFOR AND RECORDING MEDIUM FOR PROGRAMMING AND RECORDING THE SAME METHOD**

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the leakage or illegal use of information by operating and managing the security function of a portable information terminal only by access from a personal computer without operating it by the portable information terminal itself.

SOLUTION: A portable information terminal 3 receives a request for access to security related information from a host equipment 1, certifies identification information recorded in a recording medium 11 provided on the host equipment 1 and a unique identification number (non-volatile recording medium 33) provided on the portable information terminal, and permits or rejects the access according to the certified result, and communicates it to the host equipment 1. Thus, access is performed from the outside by using this so that the deletion of the secret information of a portable information terminal equipment whose location is unknown due to robbery, the report of a robber's information, and transition to a state incapable of use can be attained.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-184756

(43)公開日 平成11年(1999) 7月9日

(51)Int.Cl.⁶

G 0 6 F 12/14

識別記号

3 2 0

F I

G 0 6 F 12/14

3 2 0 A

3 2 0 D

審査請求 未請求 請求項の数33 O L (全 22 頁)

(21)出願番号

特願平9-357756

(22)出願日

平成9年(1997)12月25日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 野瀬 正毅

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

(72)発明者 沼尻 裕

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

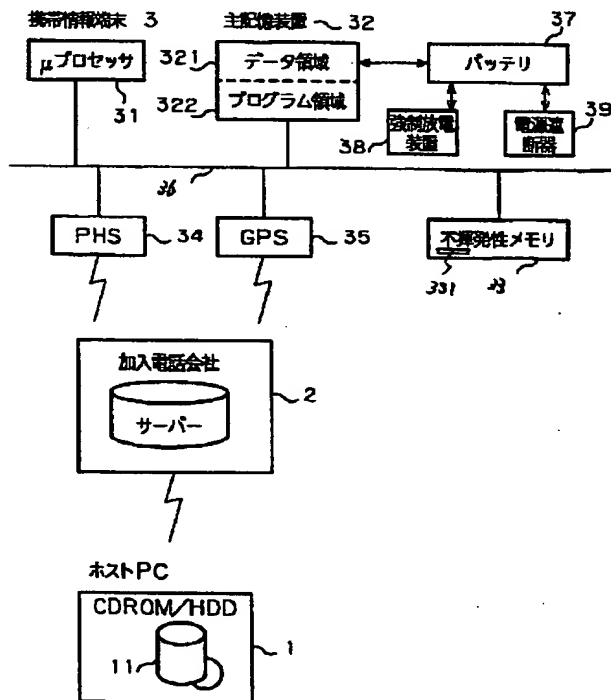
(74)代理人 弁理士 大胡 典夫 (外1名)

(54)【発明の名称】 携帯情報端末におけるセキュリティ制御方法ならびにシステム及び同方法がプログラムされ記録される記録媒体

(57)【要約】

【課題】 本発明は、携帯情報端末のセキュリティ機能をその携帯情報端末自身で操作することなく、パーソナルコンピュータからのアクセスでのみ操作管理することにより、情報の漏洩、不正使用を防止するとともに、セキュリティ機能の充実をはかることを課題とする。

【解決手段】 本発明は、携帯情報端末3において、ホスト機器1からセキュリティ関連情報のアクセス要求を受け、ホスト機器が持つ記録媒体11に記録されている識別情報と携帯情報端末が持つユニークな識別番号(不揮発性記録媒体33)との認証を行ない、認証結果によっては、アクセスを許可もしくは拒否し、ホスト機器に通知する。このことを利用し外部からアクセスすることで盗難による所在不明な携帯情報端末の機密情報削除、盗難者情報の通知、使用不能状態への移行を行なう。



【特許請求の範囲】

【請求項 1】 自身でアクセスできない隠蔽した機密情報ファイルを含む記録媒体を持つ携帯情報端末であって、携帯情報端末毎付されるユニークな識別情報と同一、もしくは対応する識別情報を持つホスト機器によってのみ上記機密情報ファイルのアクセスを許可することを特徴とするセキュリティ制御方法。

【請求項 2】 携帯情報端末において、ホスト機器からセキュリティ関連情報のアクセス要求を受け、ホスト機器が持つ記録媒体に記録されている識別情報と携帯情報端末が持つユニークな識別番号との認証を行ない、認証結果によっては、上記のアクセスを許可もしくは拒否し、ホスト機器に通知することを特徴とするセキュリティ制御方法。

【請求項 3】 携帯情報端末が持つ識別情報と同一、もしくは対応する識別情報を持つホスト機器から一定期間以上アクセスが無い場合に不正使用と判断することを特徴とする請求項 2 記載のセキュリティ制御方法。

【請求項 4】 初期設定時において隠蔽された情報ファイルと同一もしくは共通のデータが格納され、携帯情報端末からアクセス可能な開放された情報ファイルと、携帯情報端末が持つ記録媒体に記録された隠蔽された機密情報ファイルの内容を比較し、その結果によっては不正使用と判断することを特徴とする請求項 2 記載のセキュリティ制御方法。

【請求項 5】 不正使用である旨の通知をうけたとき、携帯情報端末が持つ記録媒体のバックアップのための電源を遮断し、記録情報を消去することを特徴とする請求項 3 または 4 記載のセキュリティ制御方法。

【請求項 6】 携帯情報端末からの要求に従い、携帯情報端末が持つ記録媒体のバックアップのための電源を遮断し、記録情報を消去することを特徴とする請求項 5 記載のセキュリティ制御方法。

【請求項 7】 不正使用である旨の通知をうけたとき、携帯情報端末が持つ記録媒体のバックアップのための電源を強制放電し、記録情報を消去することを特徴とする請求項 3 または 4 記載のセキュリティ制御方法。

【請求項 8】 携帯情報端末からの要求に従い、携帯情報端末が持つ記録媒体のバックアップのための電源を遮断し、記録情報を消去することを特徴とする請求項 7 記載のセキュリティ制御方法。

【請求項 9】 ホスト機器が携帯情報端末に対して通信回線を介して接続要求を發し、所有者からの通信であるか否かを上記識別情報の比較によって認証を行ない、通信回線を介して到来するコマンドを受信してそのコマンドに従うセキュリティを実行することを特徴とする請求項 1 記載のセキュリティ制御方法。

【請求項 10】 加入している電話会社に対し、加入通信機器を含む携帯情報端末の発信位置情報を要求し、当該携帯情報端末の通信機が使用中であれば受信局の特定

により概略使用位置情報を得ることを特徴とする請求項 9 記載のセキュリティ制御方法。

【請求項 11】 個々にユニークな識別情報が付され、自身でアクセスできない隠蔽された機密情報ファイルを含む記録媒体を持つ携帯情報端末と、上記識別情報に対応する識別情報を含み、上記携帯情報端末と協働して上記機密情報ファイルのアクセスを行なうホスト機器が通信回線を介して接続されて成ることを特徴とする携帯情報端末におけるセキュリティ制御システム。

10 【請求項 12】 上記携帯情報端末は、識別番号があらかじめ書き込まれ、自身でアクセスできない不揮発性メモリと、上記識別情報と同一、もしくは対応する識別情報を持つホスト機器によってアクセスされ、自身でアクセスできない隠蔽された機密情報ファイルを含む記録媒体とを具備することを特徴とする請求項 11 記載のセキュリティ制御システム。

【請求項 13】 記録媒体の記憶内容のバックアップを行なうバックアップ電源を更に具備することを特徴とする請求項 11 記載のセキュリティ制御システム。

20 【請求項 14】 外部からの指示によりバックアップ電源の遮断を行なうか、強制放電を行なう電源制御装置を更に具備することを特徴とする請求項 11 記載のセキュリティ制御システム。

【請求項 15】 ホスト機器との通信を確立する携帯電話を更に具備することを特徴とする請求項 11 記載のセキュリティ制御システム。

【請求項 16】 ホスト機器からの要求に基づき発信位置を通知する GPS 受信機を更に具備することを特徴とする請求項 15 記載のセキュリティ制御システム。

30 【請求項 17】 上記ホスト機器は、携帯情報端末が持つ識別情報と同一もしくは対応する識別情報を持ち、携帯情報端末と協働して携帯情報端末が持つ機密情報ファイルをアクセスするプログラムが格納される記録媒体を具備することを特徴とする請求項 11 記載のセキュリティ制御システム。

【請求項 18】 自身でアクセスできない隠蔽した機密情報ファイルを含む記録媒体を持つ携帯情報端末において用いられ、外部接続されるホスト機器から上記機密情報ファイルに対するアクセス要求を受け付けるステップと、ホスト機器の識別情報を読み込むステップと、携帯情報端末が持つ識別情報と上記ホスト機器の識別番号を比較して同じ、もしくは対応関係にあるか否かを判断するステップと、上記比較の結果によっては携帯情報端末の機密情報ファイルへのアクセスを許可、もしくは拒否することをホスト機器に通知するステップとがプログラムされ記録されるコンピュータ読み取り可能な記録媒体。

50 【請求項 19】 隠蔽された機密情報ファイルのアクセス要求を受信するステップと、携帯情報端末からの要求であったときそのアクセスを拒否し、否であったときホ

スト機器からの要求であることを確認し、識別情報のマッチング検査を行ないホスト機器から機密情報ファイルのアクセスを実行するステップとがプログラムされ記録される請求項18記載のコンピュータ読み取り可能な記録媒体。

【請求項20】 携帯情報端末に記録された、前回ホスト機器によりアクセスされた時刻情報を読み取るステップと、現在日時と上記時刻情報を比較し、所定の時間以上アクセスがなかったことを検査するステップと、検査の結果によりアクセス時刻情報を更新、もしくは不正使用と判断して外部へ通知するステップとがプログラムされ記録される請求項18記載のコンピュータ読み取り可能な記録媒体。

【請求項21】 隠蔽された機密情報ファイルの内容を参照するステップと、初期設定時において隠蔽された情報ファイルと同一もしくは共通のデータが格納され、携帯情報端末からアクセス可能な開放された情報ファイルの内容を参照するステップと、隠蔽された情報ファイルと開放された情報ファイルの対応する項目の内容の一致を検査するステップと、検査結果によっては不正使用と判断し、外部へ通知するステップとがプログラムされ記録される請求項18記載のコンピュータ読み取り可能な記録媒体。

【請求項22】 不正使用を検知することにより起動され、携帯情報端末の記録媒体のバックアップ電源を遮断すべく指示を発するステップがプログラムされ記録される請求項21記載のコンピュータ読み取り可能な記録媒体。

【請求項23】 不正使用を検知することにより起動され、携帯情報端末が持つ記録媒体のバックアップ電源に対し強制放電を指示するステップがプログラムされ記録される請求項21記載のコンピュータ読み取り可能な記録媒体。

【請求項24】 不正使用の通知を受けフラグをセットするステップと、通信コネクションを確立することにより起動され、フラグを参照するステップと、フラグがセットしていたとき、隠蔽された機密情報ファイルに格納されたアドレス先に、開放された情報ファイルの内容を電子メールで送付するステップとがプログラムされ記録される請求項21記載のコンピュータ読み取り可能な記録媒体。

【請求項25】 不正使用を検知することにより起動され、割り込み禁止状態に設定するステップと、携帯情報端末が持つ記録媒体の全てのファイル、もしくは事前に指定したファイルの内容を強制削除するステップとがプログラムされ記録される請求項21記載のコンピュータ読み取り可能な記録媒体。

【請求項26】 携帯情報端末の表示画面に開放された情報ファイルの内容を表示するステップと、その情報ファイルに対する変更要求を受け付け、エディタを起動し

て編集処理を行なうステップと、変更要求がないとき、あるいは編集処理終了後にその表示を閉じるステップとがプログラムされ記録される請求項18記載のコンピュータ読み取り可能な記録媒体。

【請求項27】 ホスト機器が携帯情報端末に対し通信回線を介して接続要求を発することにより起動され、所有者からの通信であるか否か上記識別情報のマッチング検査によつて認証するステップと、通信回線を介してコマンドを受信し、セキュリティ機能を起動するステップと、コマンドに従うセキュリティを実行するステップとがプログラムされ記録されるコンピュータ読み取り可能な請求項18記載の記録媒体。

【請求項28】 セキュリティモードにあることを検査するステップと、リモートロックを行なうコマンドを受信するステップと、携帯情報端末をロックするステップとがプログラムされ記録される請求項27記載のコンピュータ読み取り可能な記録媒体。

【請求項29】 通信回線を介して警告音を発するコマンドを受信するステップと、携帯情報端末から警告音の発生を指示するステップとがプログラムされ記録される請求項27記載のコンピュータ読み取り可能な記録媒体。

【請求項30】 携帯情報端末にGPS受信機が装備されていることを検査するステップと、GPS受信機を介して現在位置を通知するステップとが更にプログラムされ記録される請求項27記載のコンピュータ読み取り可能な記録媒体。

【請求項31】 データを消去するコマンドを受信するステップと、携帯情報端末が持つ記録媒体に記録されている情報を消去するステップとが更にプログラムされ記録される請求項27記載のコンピュータ読み取り可能な記録媒体。

【請求項32】 識別情報のマッチングによる認証に従い、携帯情報端末に対するプログラムの再インストールを許可するステップが更にプログラムされ記録される請求項27記載のコンピュータ読み取り可能な記録媒体。

【請求項33】 加入している電話会社に対し、加入通信機器を含む携帯情報端末の発信位置情報を要求するステップと、当該携帯情報端末の通信機が使用中であれば受信局の特定により概略使用位置情報を得るステップとがプログラムされ、記録される請求項18記載のコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、携帯情報端末におけるセキュリティ制御方法ならびにシステム及び同方法がプログラムされ記録される記録媒体に関する。

【0002】

【従来の技術】 半導体技術の進歩に伴い携帯情報端末が普及してきた。携帯情報端末はパーソナルユースがほと

んどであり、従って、業務情報の他にプライバシー情報も扱うことが多く、収納データに対するセキュリティ保護が望まれていた。

【0003】また、携帯情報端末は、社内や自宅で使用する他、携帯して外で使うことができることから盗難や紛失する可能性もある。しかしながら、情報漏洩を防ぐための手段や盗難を抑止するための手段はほとんど講じられていないのが現状である。携帯情報端末は、その性格上廉価構成をとることがのぞまれ、従って、基本性能ではないセキュリティのために特別な機能を装置に付加することは困難であった。

【0004】

【発明が解決しようとする課題】電子手帳から発展した携帯情報端末は共用することを前提としていないため、ほとんどがセキュリティ機能を装備していない。また、パーソナルコンピュータから発展し、小型化された携帯情報端末は、ブートメディアを使用して立ち上げることでパスワードを回避して使用することが可能である。

【0005】一方、ネットワークコンピュータやPHS内蔵の情報端末が登場したが、パスワードによるセキュリティのみで、能動的に情報漏洩を防ぐ機能は用意されていない。将来的にデファクトスタンダードになると予測されるハンドヘルドコンピュータが1996年末米国で発売され、1997年夏から国内でも販売が開始されたが、その中に十分なセキュリティ機能は搭載されていない。この種携帯情報端末に格納された情報は、他の全ての携帯情報端末によりアクセスすることができるため、有効なセキュリティ機能の実現が困難であった。

【0006】携帯情報端末は、基本的に単体で用いることは少なくパーソナルコンピュータと連係して使用することが多い。そこで、携帯情報端末のセキュリティ機能をその携帯情報端末自身で操作することなく、パーソナルコンピュータからのアクセスでのみ操作管理することにより、情報の漏洩、不正使用を防止するとともに、セキュリティ機能の充実をはかった携帯情報端末におけるセキュリティ制御方法ならびに装置及び同方法がプログラムされ記録される記録媒体を提供することを目的とする。

【0007】

【課題を解決するための手段】本発明の携帯情報端末におけるセキュリティ制御方法は、自身でアクセスできない隠蔽された機密情報ファイルを含む記録媒体を持つ携帯情報端末であって、携帯情報端末毎付されるユニークな識別情報と同一、もしくは対応する識別情報を持つホスト機器によってのみ上記機密情報ファイルのアクセスを許可することを特徴とする。また、携帯情報端末において、ホスト機器からセキュリティ関連情報のアクセス要求を受け、ホスト機器が持つ記録媒体に記録されている識別情報と携帯情報端末が持つユニークな識別番号との認証を行ない、認証結果によっては、上記のアクセスを

許可もしくは拒否し、ホスト機器に通知することも特徴とする。

【0008】本発明のセキュリティ制御システムは、個々にユニークな識別情報が付され、自身でアクセスできない隠蔽された機密情報ファイルを含む機密情報ファイルを含む記録媒体を持つ携帯情報端末と、上記識別情報に対応する識別情報を含み、上記携帯情報端末と協働して上記機密情報ファイルのアクセスを行なうホスト機器が通信回線を介して接続されて成ることを特徴とする。

【0009】本発明の記録媒体は、自身でアクセスできない隠蔽した機密情報ファイルを含む記録媒体を持つ携帯情報端末において用いられ、外部接続されるホスト機器から上記機密情報ファイルに対するアクセス要求を受け付けるステップと、ホスト機器の識別情報を読み込むステップと、携帯情報端末が持つ識別情報と上記ホスト機器の識別番号を比較して同じ、もしくは対応関係にあるか否かを判断するステップと、上記比較の結果によっては携帯情報端末の機密情報ファイルへのアクセスを許可、もしくは拒否することをホスト機器に通知するステップとがプログラムされ記録されることを特徴とする。

【0010】上述した携帯情報端末におけるセキュリティ制御方法ならびに装置及び同方法がプログラムされ記録される記録媒体を用い、不正使用を検知し、また、電源遮断による情報漏洩の防止、あるいは強制放電による情報漏洩防止、電子メールによる自動情報通知、更には、ホスト機器からのアクセスによるセキュリティリモートコントロール、リモートロック、リモート警告音発生、リモート所在通知、リモートデータ消去、リモートアクセス認証、携帯情報端末盗難時に加入電話会社による位置情報を取得することにより、充実したセキュリティ機能を実現できる。

【0011】

【発明の実施の形態】図1は本発明の実施形態を示すブロック図である。図において、符号1は、ホストとなるパーソナルコンピュータであり、電話会社2が管理する回線経由で携帯情報端末3が接続される。

【0012】携帯情報端末は、制御中枢となるマイクロプロセッサ31、プログラム乃至データが格納される記録媒体32、不揮発性メモリ33、通信媒体となるPHS34、あるいはGPS35がバス36を介して共通接続される。記録媒体32は、データ領域321とプログラム領域322から成り、各領域に割り付けられるデータ、プログラムについては図2で詳述する。不揮発性メモリ33には携帯情報端末の識別情報331が記録される。37は記録媒体32の記憶内容保持のために使用される電源バッテリーであり、更に、ある条件の下で強制放電させる強制放電装置38、電源供給を遮断する電源遮断器39が組込まれている。

【0013】図2は、図1における記録媒体に割り付けられ格納されるデータやプログラムを記録媒体上に展開

して示した図である。

【0014】データ領域321には、所有者の氏名、住所、電子メールアドレス、電話番号、パスワード等の機密情報が格納される。秘蔵したい機密情報ファイル3211、対応するパーソナルコンピュータに接続される毎に更新され、携帯情報端末からは変更できない接続情報3212、使用者の氏名、住所、電話番号、電子メールアドレス等リードライト可能な個人情報ファイル3213がデータ領域に割り付けられ記録される。

【0015】また、プログラム領域322には、不正使用検知プログラム3221、3222、電源遮断プログラム3223、個人情報表示&変更プログラム3224、記録媒体強制削除プログラム3225、インターネット接続検知プログラム3226、自動情報通知プログラム3227、パスワード要求プログラム3228、強制情報削除プログラム3229、リモートロックプログラム3230、リモート警告音発生プログラム3231、リモート所在通知プログラム3232、リモートデータ消去プログラム3233、リモートアクセス認証プログラム3234、インストール管理プログラム3235、機密情報ファイル変更プログラム3236がそれぞれ割り付けられ記録される。

【0016】不正使用検知プログラム3221は、接続履歴が一定期間以上更新されなかったときに不正使用であると識別するために用意される。不正使用検知プログラム3222は、秘蔵した機密情報ファイル3211と個人情報ファイル3213の内容を比較し、不一致のときに不正使用であると識別するために用意される。

【0017】電源遮断プログラム3223は、不正使用の通知を受けると電源遮断装置39を用いて携帯情報端末3の記録媒体32の記憶保持のために使用される電源供給を遮断して情報を消去するために用意される。個人情報表示&変更プログラム3224は、個人情報ファイル3213の内容を携帯情報端末3の画面に表示し、また、変更要求を受け付け、個人情報ファイル3213の内容を変更するために用意される。記憶媒体強制削除プログラム3225は、携帯情報端末3の記憶媒体32に記憶されるデータを強制的に削除するために用意される。

【0018】インターネット接続検知プログラム3226は、ネットワークプロトコル、あるいはネットワークデバイスドライバ等通信リソースを管理し、電子メールの送信が可能か否かを関しするために用意される。自動情報通知プログラム3227は、インターネットを用いて秘蔵した機密情報ファイル3211に記録したアドレスへ、個人情報ファイル3213の情報を電子メールによって自動送信するために用意される。

【0019】パスワード要求プログラム3228は、携帯情報端末3がレジューム等休止の状態から復帰する際に、パスワード入力を要求し、不一致の場合に稼動状態

に移行させないために用意される。強制情報削除プログラム3229は、不正使用の通知を受けた場合にバッテリーの強制放電装置38を用いて記録媒体32の記憶保持のために使用されるバッテリー37を強制放電し、情報を消去するために用意される。

【0020】リモートロックプログラム3230は、遠隔地にあるホストパーソナルコンピュータ1より、後述するセキュリティリモートコントロールプログラム115の要求を受け、携帯情報端末3の電話受信機能以外の入出力機能をロックするために用意される。リモート警告音発生プログラム3231は、遠隔地にあるホストパーソナルコンピュータ1より、セキュリティリモートコントロールプログラム115の要求を受け、音声や警告音を発生するために用意される。リモート所在通知プログラム3232は、遠隔地にあるホストパーソナルコンピュータ1より、セキュリティリモートコントロールプログラム115の要求を受け、携帯情報端末3に接続するGPS35より現在地を求めホストパーソナルコンピュータ1へ通知するために用意される。

【0021】リモートデータ消去プログラム3233は、遠隔地にあるホストパーソナルコンピュータ1より、セキュリティリモートコントロールプログラム115の要求を受け、携帯情報端末3の記録媒体32の情報を強制削除するために用意される。リモートアクセス認証プログラム3234は、遠隔地にあるホストパーソナルコンピュータ1より、セキュリティリモートコントロールプログラム115を介してアクセス要求を受けた場合、要求に含まれる後述する識別情報と携帯情報端末3の不揮発性メモリ33に内蔵の識別情報331のマッチングをとり、不一致の場合にはセキュリティリモートコントロールプログラム115の要求を拒否するために用意される。

【0022】インストール管理プログラム3235は、携帯情報端末3にプログラムをインストールする際に使用されるインストーラで、識別情報と識別情報331のマッチングをとり、不一致の場合にはインストールを拒否するために用意される。機密情報ファイル変更プログラム3236は変更要求に含まれる後述する識別情報と携帯情報端末3にある識別番号313のマッチングをとり、一致したときに秘蔵した機密情報ファイル3211の内容を読み書きするために用意される。

【0023】ホストパーソナルコンピュータ1は、CD-ROMもしくはハードディスク等の記録媒体11を有し、ホストパーソナルコンピュータ1にユニークな識別番号111が記録される他、記録媒体32に含まれる秘蔵した機密情報ファイル321をリードライトするためのアクセスプログラム112、記録媒体11に含まれる識別情報111と携帯情報端末3の識別情報331とのマッチングをとり、不一致のときにはアクセスを拒否する認識プログラム113、対応する携帯情報端末3と接

続したときにその携帯情報端末 3 にある接続履歴情報 322 を更新する接続情報更新プログラム 114、PHS、GPS 等無線電話による通信媒体を介して携帯情報端末 3 にアクセスし、携帯情報端末 3 が持つリモートセキュリティ機能を制御するセキュリティリモートコントロールプログラム 115、携帯情報端末 3 にソフトウェアをインストールする際に使用され、識別情報 111 と識別情報 331 のマッチングをとって不一致のときにインストールを拒否するインストーラ 116、加入電話会社 2 の当該サーバにアクセスし、加入電話が使用中である場合には使用位置情報をアクセスして表示する位置情報取得プログラム 117 が割り付けられ記憶される。

【0024】図 3～図 2 は本発明実施形態の動作を説明するために引用したフローチャートであり、それぞれが本発明により用意される各プログラムの実行手順を示す。

【0025】以下、図 3～図 2 に示すフローチャートを参照しながら、図 1、図 2 に示す本発明実施形態の動作について詳細に説明する。

【0026】まず、携帯情報端末 3 の立ち上げから説明する。電源 OFF 状態または、休止状態にある携帯情報端末 3 を稼動状態に移行するためには、パスワード要求プログラム 3227 が割り込み禁止状態となっておりときに携帯情報端末 3 を起動する必要がある。携帯情報端末 3 が持つ入力装置を介して入力されたパスワードを、隠蔽した機密情報ファイル 3211 に記録されたパスワードと比較し、一致したときに優先度を元に戻して稼動状態へ移行する。パスワードが一致しなかった場合は、優先度を元に戻してレジューム状態に移行する。

【0027】ここで、隠蔽した機密情報ファイル 3211 の変更操作について図 4 に示すフローチャートを参照しながら説明する。隠蔽した機密情報ファイル 3211 は、携帯情報端末 3 から直接読み書きを行なえないような細工をしてある。所有者は、ホストパーソナルコンピュータ 1 から、携帯情報端末 3 にある不揮発性メモリ 33 に内蔵された識別情報 331 と一致する識別情報 111 を持つ記憶媒体 11 に割り付け格納済みの、隠蔽した機密情報ファイルのアクセスプログラム 112 を起動する。ここで、ホストパーソナルコンピュータ 1 と接続された携帯情報端末 3 は、機密情報ファイル変更プログラム 3236 を起動して上述した機密情報ファイルアクセスプログラム 112 の要求に含まれる識別情報 111 と携帯情報端末の不揮発性メモリ 33 に記録されてある識別情報 331 の内容を比較（ステップ S3）し、一致すれば隠蔽した機密情報ファイルアクセスプログラム 112 の変更内容入力受付ルーチンを起動し、使用者に変更内容の入力を促す。変更内容が入力されると、機密情報ファイル変更プログラム 3236 は、隠蔽した機密情報ファイル 3211 の変更処理（ステップ S4）を行なう。

【0028】ホストパーソナルコンピュータ 1 からのセキュリティ機能制御について図 3 に示すフローチャートを用いて説明する。ホストパーソナルコンピュータ 1 から携帯情報端末 3 のセキュリティ関連プログラム 3221～3236 を起動するとき、認識プログラム 113 により識別情報 111 と携帯情報端末 3 が持つ識別情報 331 の一致を確認（ステップ S3）する。ここで一致が認められたときに要求のあったセキュリティ関連プログラムを起動（ステップ S4）し、不一致であればセキュリティ機能関連の制御を拒否（ステップ S5）する。

【0029】次に、本発明の特徴の一つである接続履歴情報による不正使用の検知操作について図 5 に示すフローチャートを参照しながら説明する。接続履歴更新プログラム 114 は、ホストパーソナルコンピュータ 1 と携帯情報端末 3 が接続されたときに呼び出され、上述した認識プログラム 113 をコールして識別情報 111 と識別情報 331 の一致確認を行なう。ここで一致が認められたときに携帯情報端末 3 の記録媒体 31 に格納される接続履歴情報ファイル 3212 を更新する。不正使用検知プログラム 3221 は、システム稼動時におけるトリガを利用して起動（ステップ S1）され、接続履歴情報ファイル 3212 を参照し、現在日時と前回のアクセス日時を比較（ステップ S3）して一定時間以上更新されなければ不正に使用されていると判断（ステップ S4）する。

【0030】一方、個人情報の矛盾による不正使用の検知について図 6 に示すフローチャートを参照しながら説明する。携帯情報端末 3 は上述した起動時等におけるトリガを利用して個人情報表示 & 変更プログラム 3227 を起動する。このプログラム 3227 では、容易に表示情報を変更できるように、情報変更画面を設ける。不正な使用者がこの情報を変更した場合、携帯情報端末 3 の隠蔽した機密情報ファイル 3211 の内容との矛盾が生じる。これによって不正使用を検知する。通常、正規の利用者が隠蔽した機密情報ファイル 3211 の内容を変更した場合には、携帯情報端末 3 と対をなす記録媒体 11 に格納された機密情報ファイル更新プログラム 114 を用いる。

【0031】次に、本発明の特徴の一つである電源遮断による情報消去により情報漏洩を防止するための方法について、図 7、図 8 に示すフローチャートを参照しながら述べる。図 7 に示すフローチャートにおいて、上述した不正使用検知プログラム 3221 あるいは 3222 により不正使用が通知（ステップ S71）されると、電源遮断プログラム 3223 は、電源遮断装置 39 を制御して携帯情報端末 3 の記録媒体 32 における記憶保持のための電源を遮断（ステップ S72）し、情報の消去をはかる。

【0032】一方、図 8 に示すフローチャートにおいて、ステップ S81 で不正使用が通知されると、記憶媒

体強制削除プログラム3225により優先度を最高レベルに設定して割り込み禁止とし(ステップS82)、携帯情報端末3の記録媒体32のファイルの全てを強制削除、あるいは事前に指定したファイルのみ強制削除する(ステップS83)ことも考えられる。

【0033】次に図9に示すフローチャートを参照しながら、本発明の特徴の一つである強制放電による情報漏洩防止方法について詳述する。不正使用検知プログラム3221、あるいは3222により不正使用が検知されることにより強制情報削除プログラム3229がコール(ステップS91)される。このとき、強制情報削除プログラム3229は、バッテリー強制放電装置38をコントロール(ステップS92)することにより、携帯情報端末3の記録媒体31の記憶内容保持のために供給されているバッテリー31を強制放電し、情報を消去する。

【0034】ところで、個人情報の表示&変更プログラム3224は、携帯情報端末3の表示画面に公開された情報ファイルの内容を表示し、その情報ファイルに対する変更要求を受け付ける。そして、変更要求を受け付けるアイコンもしくはボタン等を使用者が操作したかチェックし、読み書き可能な個人情報ファイル3213を変更するためのエディタを展開する。このエディタを使用して編集処理を行ないエディタを閉じることにより本処理を終了する。変更要求がないとき、あるいは編集処理終了後にその表示を閉じる。

【0035】次に、本発明の特徴の一つである不正使用者情報の電子メールによる通知について、図10に示すフローチャートを参照しながら説明する。まず、不正使用検知プログラム3222により不正使用が検知され、このことが通知されると、不正使用であることを示すフラグをONする(ステップS101)。後述するインターネット接続を検知する方法により接続が通知されると、インターネット接続検知プログラム3226が起動(ステップS102)され、インターネット接続検知プログラム3226は電子メール送出可能であることを検知すると先のフラグを確認(ステップS103)し、フラグがONしていることにより、電子メールによる自動情報通知プログラム3227をコールする。自動情報通知プログラム3227は、隠蔽した機密情報ファイル3211に記録された本来の所有者のアドレスに対し、個人情報ファイル3213の内容を電子メールで自動送信する(ステップS104)。このとき、メールの送信を携帯情報端末保持者に通知しない。このことにより、本来の所有者は盗難者が入力した個人情報を知ることができる。

【0036】インターネット接続を通知する方法は図11にフローチャートで示されている。即ち、携帯情報端末3のダイヤルプロパティを設定する際、コネクションを確立した後、インターネット接続検知プログラム3226へ通知するように自動設定(ステップS111)する。そして、通信プロトコルを実現するプログラムにおいて

コネクションの確立を検出し、その旨通知(ステップS112, S113)するものである。

【0037】次に、パスワード要求プログラム3228による、携帯情報端末3が休止状態から復帰するときのパスワードブロック動作について説明する。携帯情報端末3は、パワーセーブのため、一定時間アクセスがない場合レジューム状態を継続する機能を標準で持つ。この状態から復帰する際、パスワード要求プログラム3228を起動してパスワードの入力を要求する。不一致の場合は稼動状態に移行させることはない。

【0038】次に、本発明の特徴の一つであるリモートアクセス認証方法について図12に示すフローチャートを参照しながら説明する。PHS34等を介し、携帯情報端末3のリモートセキュリティ関連プログラム3230, 3231, 3232が、ホストパーソナルコンピュータ1のセキュリティリモートコントロールプログラム115からアクセス要求を受信した場合(ステップS121)、その要求に含まれる識別情報111(ステップS122)と不揮発性メモリ33に登録されてある識別情報331とのマッチング(ステップS123)をとり、不一致の場合にはセキュリティリモートコントロールプログラム115の要求を拒否する。一致した場合には当該プログラムを起動(ステップS124)する。

【0039】セキュリティリモートコントロールにつき、図13～図17を参照しながら説明する。まず、リモートロックから説明する。リモートアクセス認証プログラム3234によりリモートロックプログラム3230がコールされると、携帯情報端末3の電話受信機能以外の入出力機能のロック、アンロックを行なう。

【0040】即ち、図13、図14のフローチャートにおいて、まず、リモートアクセス認証(図13)がなされる。具体的には、携帯情報端末3に対して通信回線を介して外部から接続(ステップS132)を行ない、識別情報による所有者からの通信であるか否かの認証チェック(S132)が行なわれる。ここで、一致が確認されてアクセスが許可されると、通信回線からコマンドを受け付け(ステップS133)、セキュリティ機能を起動(ステップS134, S135)する。

【0041】更に図14のフローチャートに移行して、セキュリティモードにあるか否かがチェック(ステップS141)され、通信回線経由でリモートロックを行なうコマンドを受けたか否かをチェック(ステップS142, S143)する。そしてそのコマンドに従い携帯情報端末3をロック、もしくはアンロック(ステップS144)する。

【0042】図15はリモート警告音発生方法についてその制御手順がフローチャートで示されている。リモートアクセス認証プログラム3234からリモート警告音発生プログラム3231がコールされると、盗難を通知する音声や警告音を発生させる。まず、セキュリティモ

ードになっているか検査(ステップS151)され、通信回線経由で受信したコマンドをチェック(ステップS152, 153)し、警告音発生を指示するコマンドであったときに携帯情報端末3から警告音を発生(ステップS154)させるものである。尚、この状態でレジューム状態に移行することはできない。

【0043】図16は、リモート所在地通知方法を実現するプログラムの動作手順をフローチャートで示したものである。GPSレシーバ35を装備した携帯情報端末3において、リモートアクセス認証プログラム3234からリモート所在地通知プログラム3232がコールされると、GPSを介して現在地が求められ、PHS34等通信機器を介してホストパーソナルコンピュータ1へ携帯情報端末3の位置情報を通知するものである。

【0044】リモート所在地通知プログラム3232は、セキュリティモードにあるか否かチェック(ステップS161)し、更に携帯情報端末3にGPS35が装備されているかチェック(ステップS162)し、いずれも成立したときに、GPSによる現在位置を通信回線経由で得、その情報をホストパーソナルコンピュータ1へ通知(ステップS163)する。

【0045】図17は、リモートデータ消去方法を実現するリモートデータ消去プログラムの動作手順をフローチャートで示したものである。リモートアクセス認証プログラム3234からリモートデータ消去プログラム3233がコールされると、携帯情報端末3が持つ記録媒体32に格納してある情報が強制削除される。

【0046】リモートデータ消去プログラム3234は、まず、携帯情報端末3がセキュリティモードにあるか否かをチェック(ステップS171)し、通信回線経由で受信したコマンドの解析(ステップS172, S173)を行ない、データを消去すべきコマンドであったときに、指定された範囲のデータを消去(ステップS174)する。

【0047】一方、携帯情報端末3にプログラムを再インストールすることにより、セキュリティ機能が回避されることを防ぐためにインストール管理プログラム3235が用意される。インストール管理プログラム3235は、識別情報のマッチングがとれたときのみ、再インストールを許可し、セキュリティ機能の継続した実現をはかる。

【0048】図18は、無線電話会社により位置情報を得る方法をフローチャートで示したものである。ホストパーソナルコンピュータ1は、自身で持つ位置情報取得プログラム117に従い、加入先電話会社に対し加入通信機器、即ち、ここではPHS34を含む携帯情報端末3の発信位置情報を要求する。ここで携帯情報端末3の通信機能が作動中であれば、受信局の特定によりおおまかな使用位置の特定がなされ、所有者に通知されるものである。

【0049】具体的には、加入先電話会社に対して携帯情報端末が盗難にあつた旨連絡が入る(ステップS181)ことから処理が開始され、携帯情報端末3に対して通信回線を介して外部から接続(ステップS182)がなされる。このことにより、使用した中継アンテナの位置情報を電話会社が取得(ステップS183)し、中継アンテナのサービス範囲情報が電話会社から所有者に対して通知(ステップS184)される。ここで、所有者は、警察に連絡するか否か決断(ステップS185)し、場合によってはその情報を伝達(ステップS186)することになる。

【0050】尚、上述した実施形態では、ハンドヘルドコンピュータ、ウォレットパーソナルコンピュータ、PDAにPHSを内蔵した携帯情報端末をホストパーソナルコンピュータに接続したもののみ例示したが、これに限定されるものではなく、ノートPCや、スケジューリングの機能を持つ時計や家電製品、あるいは将来、通信ネットワークに車が接続されるようになった場合、車のセキュリティに特に有効となるものである。

【0051】以上説明のように本発明は、通信機能を持つ携帯情報端末において、ホストとなるパーソナルコンピュータと協動することにより、携帯情報端末が盗難にあつた場合の機密情報の漏洩防止、使用停止、所在確認を行なうものである。また、加入電話会社との連係により、盗難にあつた携帯情報端末の所在を特定することができるものである。

【0052】

【発明の効果】以上説明のように、本発明は、携帯情報端末のセキュリティ機能を携帯情報端末自身で操作することなく、ホストとなるパーソナルコンピュータからのアクセスでのみ携帯情報端末のセキュリティ機能を操作管理するようにしたものである。この場合、特定の携帯情報端末のセキュリティ管理を特定のホストであるパーソナルコンピュータに限定することで携帯情報端末単体でセキュリティ機能を制御できないような仕組みを構築できる。また、携帯情報端末に機密情報を直接公開しないようにしたばかりでなく、その情報を能動的に消去することにより、不測の事態にあつても機密情報の漏洩を防止できる。また、通信機能を持つ携帯情報端末では、盗難の状況を本来の所有者に通知したり、あるいは遠隔操作でセキュリティ機能を制御することにより、より充実したセキュリティを実現できる。

【図面の簡単な説明】

【図1】本発明の実施形態を示すブロック図、

【図2】図1における記録媒体に記録されるプログラム乃至データをメモリ上に展開して示した図、

【図3】本発明の携帯情報端末の管理方法をフローチャートで示した図、

【図4】隠蔽した機密情報ファイルによる所有者情報保持方法をフローチャートで示した図、

15

【図5】不正使用を検知する方法をフローチャートで示した図、

【図6】不正使用を検知する他の方法を実現するための手順をフローチャートで示した図、

【図7】バックアップ電源を遮断することによる情報漏洩防止方法を実現するための手順をフローチャートで示した図、

【図8】強制情報削除による情報漏洩防止方法を実現するための手順をフローチャートで示した図、

【図9】強制放電による情報漏洩防止方法を実現するための手順をフローチャートで示した図、 10

【図10】電子メールによる自動情報通知方法を実現するための手順をフローチャートで示した図、

【図11】インターネット接続を通知する方法を実現するための手順をフローチャートで示した図、

【図12】リモートアクセス認証方法を実現するための手順をフローチャートで示した図、

【図13】セキュリティリモートコントロールの方法を実現するための手順をフローチャートで示した図、

【図14】リモートロック方法を実現するための手順をフローチャートで示した図、 20

【図15】リモート警告音発生方法を実現するための手順をフローチャートで示した図、

【図16】リモート所在地通知方法を実現するための手順をフローチャートで示した図、

【図17】リモートデータ消去方法を実現するための手順をフローチャートで示した図、

【図18】加入電話会社から位置情報を得るための方法

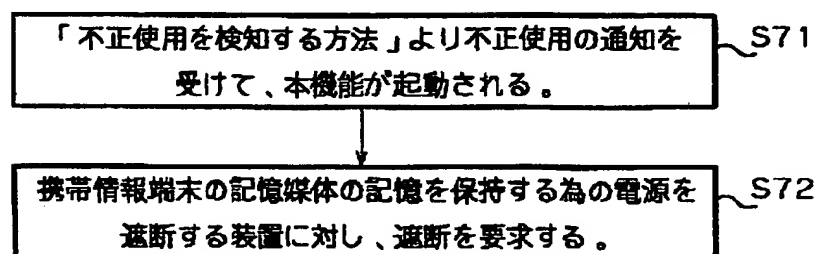
16

を実現するための手順をフローチャートで示した図、

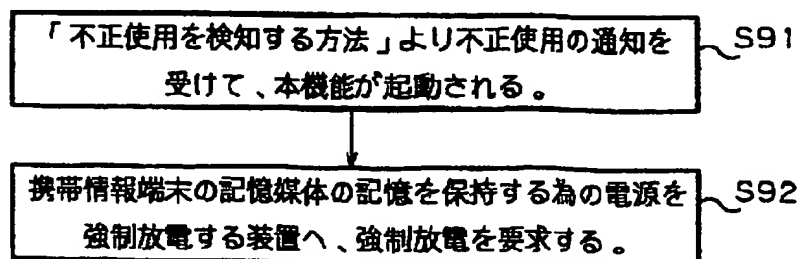
【符号の説明】

1…ホストパーソナルコンピュータ、2…電話会社（サーバ）、3…携帯情報端末、11…記録媒体（ホスト）、31…マイクロプロセッサ（CPU）、32…記録媒体（端末）、33…不揮発性記録媒体、34…PHS、35…GPS、36…バス、37…バッテリー（バックアップ）、38…強制放電装置、39…電源遮断器、111…ホスト識別情報、112…機密情報ファイル、113…認識プログラム、114…接続情報更新プログラム、115…セキュリティリモートコントロールプログラム、116…インストーラ、117…位置情報取得プログラム、321…データ領域、322…プログラム領域、3211…機密情報ファイル、3212…接続情報ファイル、3213…個人情報ファイル、3221…不正使用検知プログラムA、3222…不正使用検知プログラムB、3223…電源遮断プログラム、3224…個人情報表示&変更プログラム、3225…記録媒体強制削除プログラム、3226…インターネット接続検知プログラム、3227…自動情報通知プログラム、3228…パスワード要求プログラム、3229…強制情報削除プログラム、3230…リモートロックプログラム、3231…リモート警告音発生プログラム、3232…リモート所在地通知プログラム、3233…リモートデータ消去プログラム、3234…リモートアクセス認証プログラム、3235…インストール管理プログラム、3236…機密情報ファイル変更プログラム。

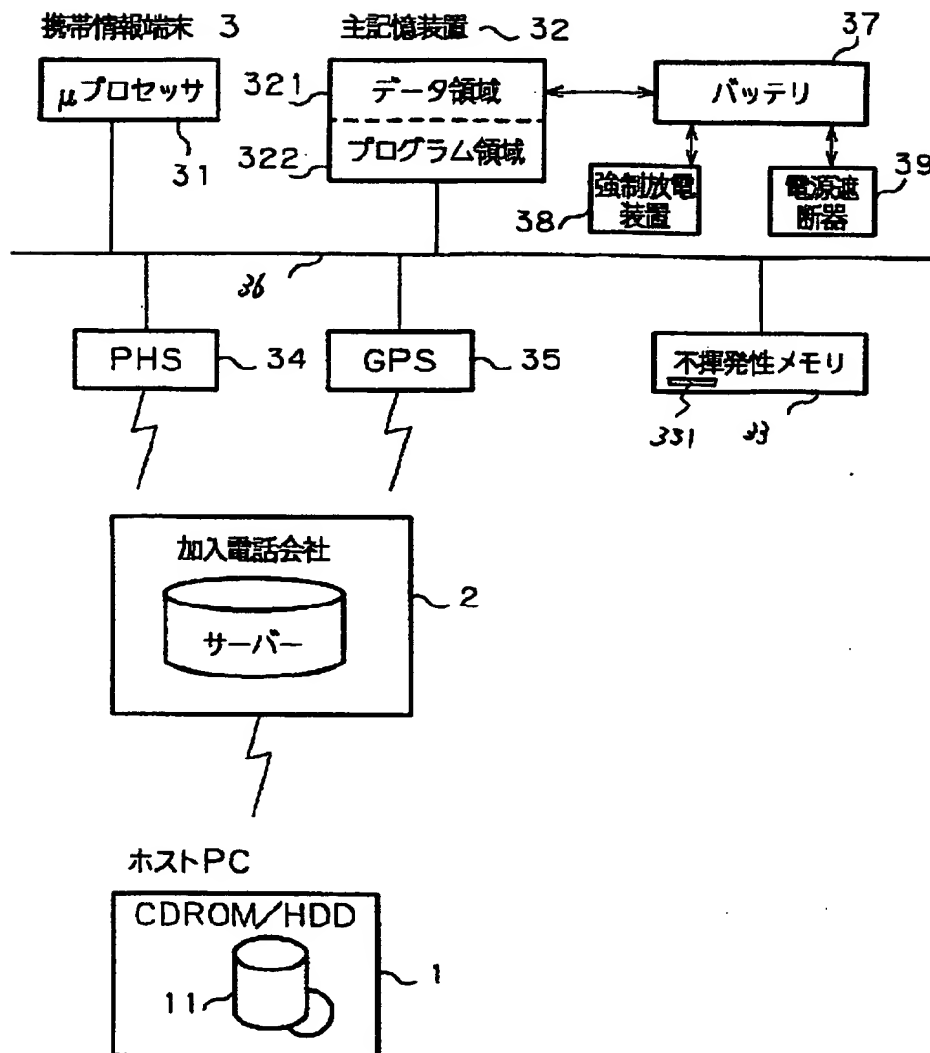
【図7】



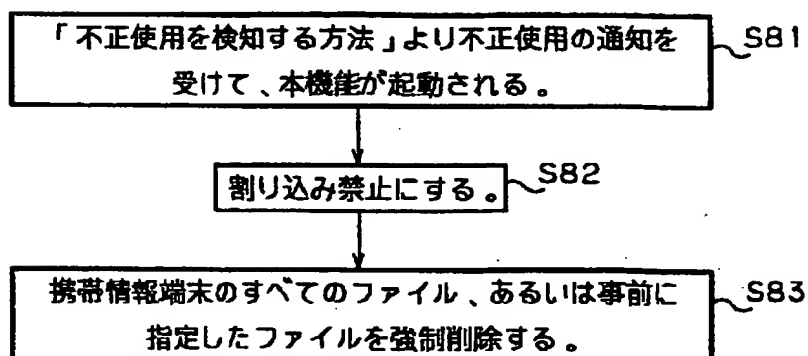
【図9】



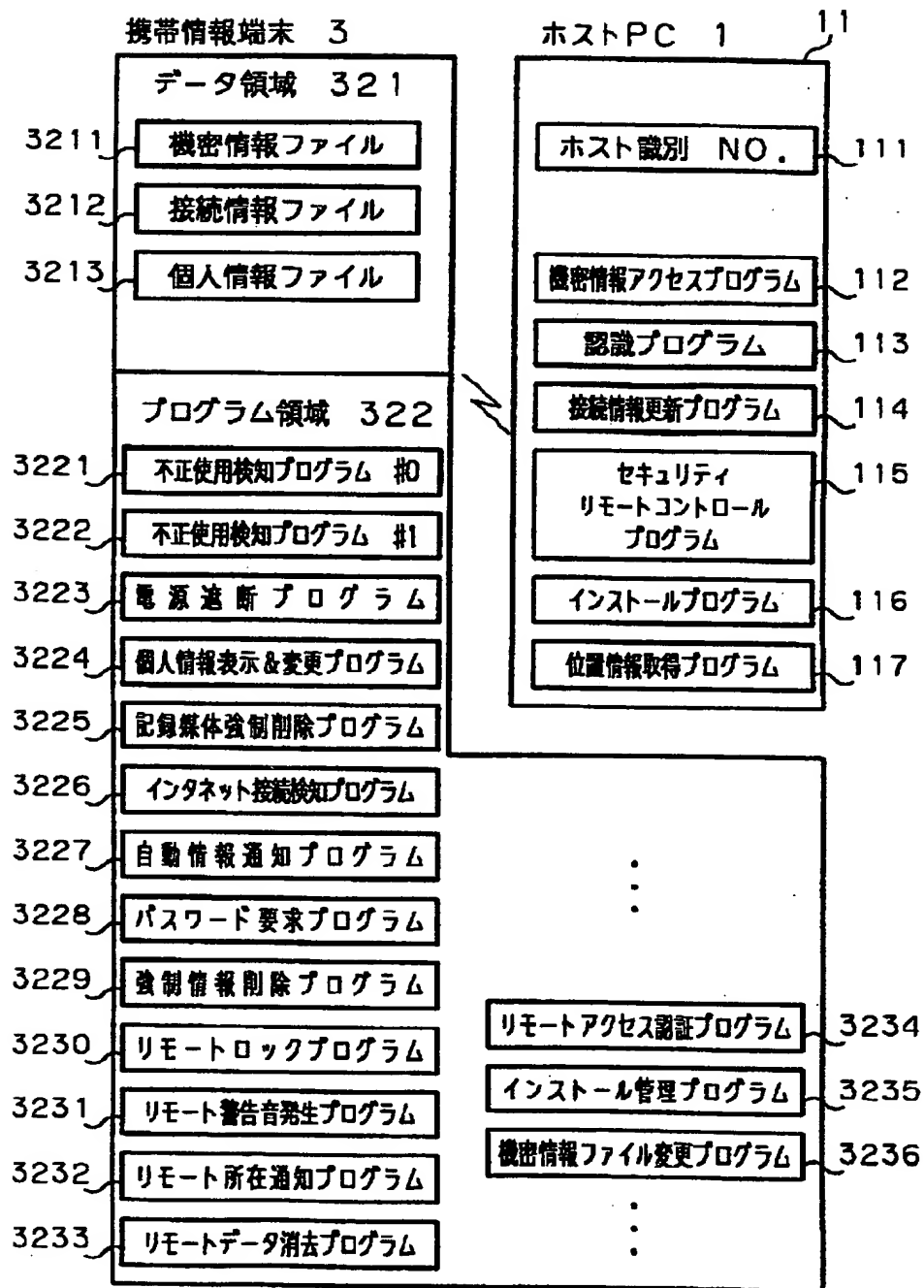
【図1】



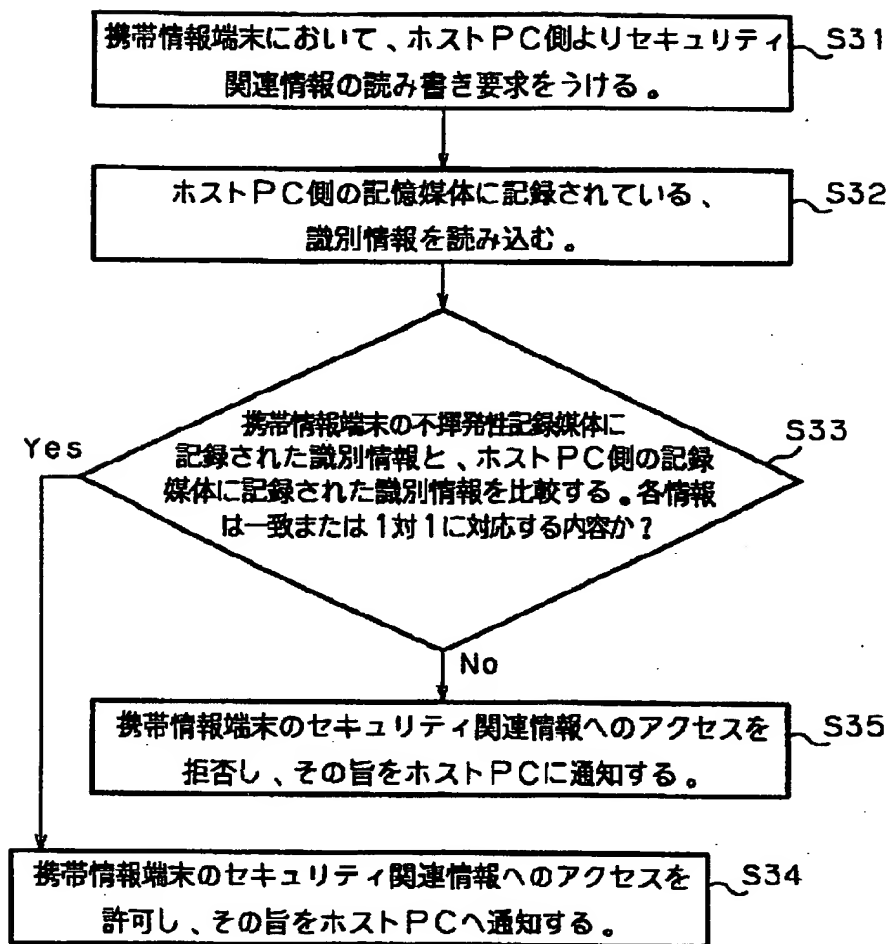
【図8】



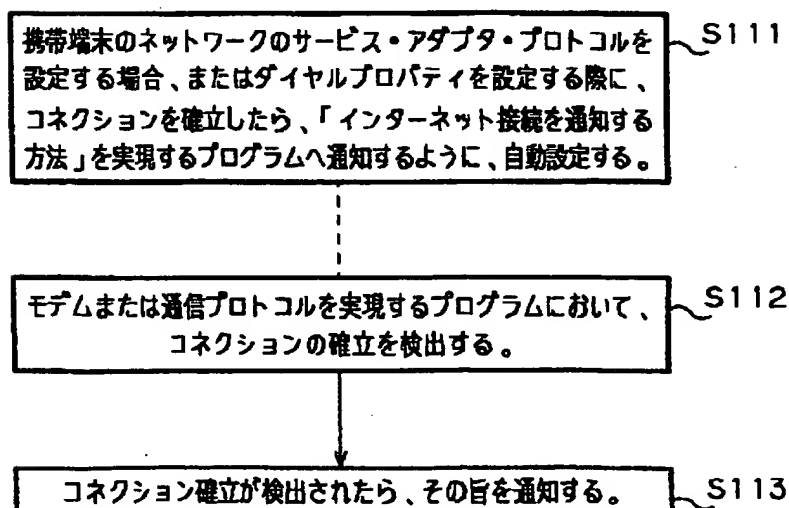
【図 2】



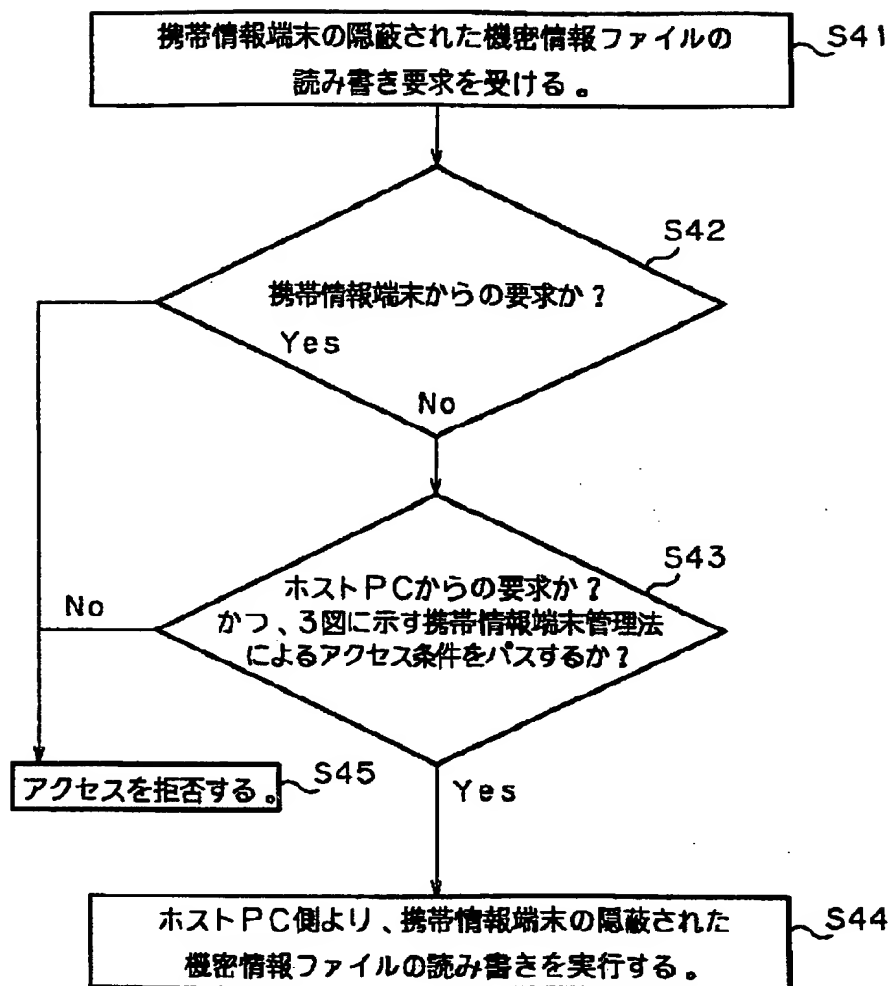
【図 3】



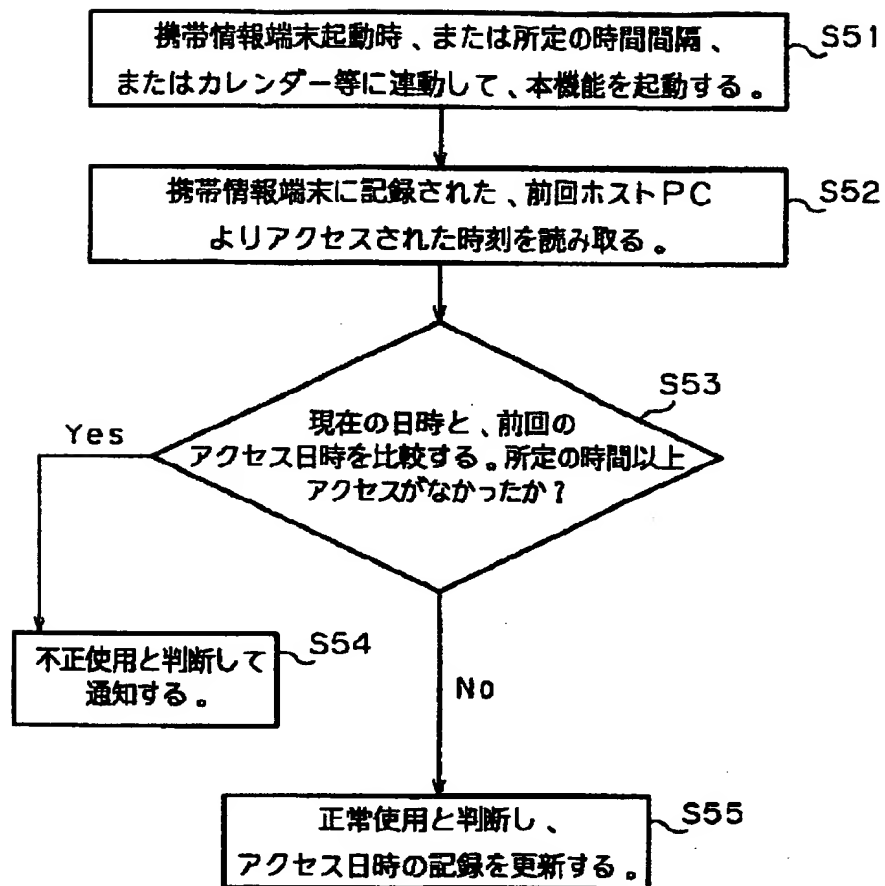
【図 11】



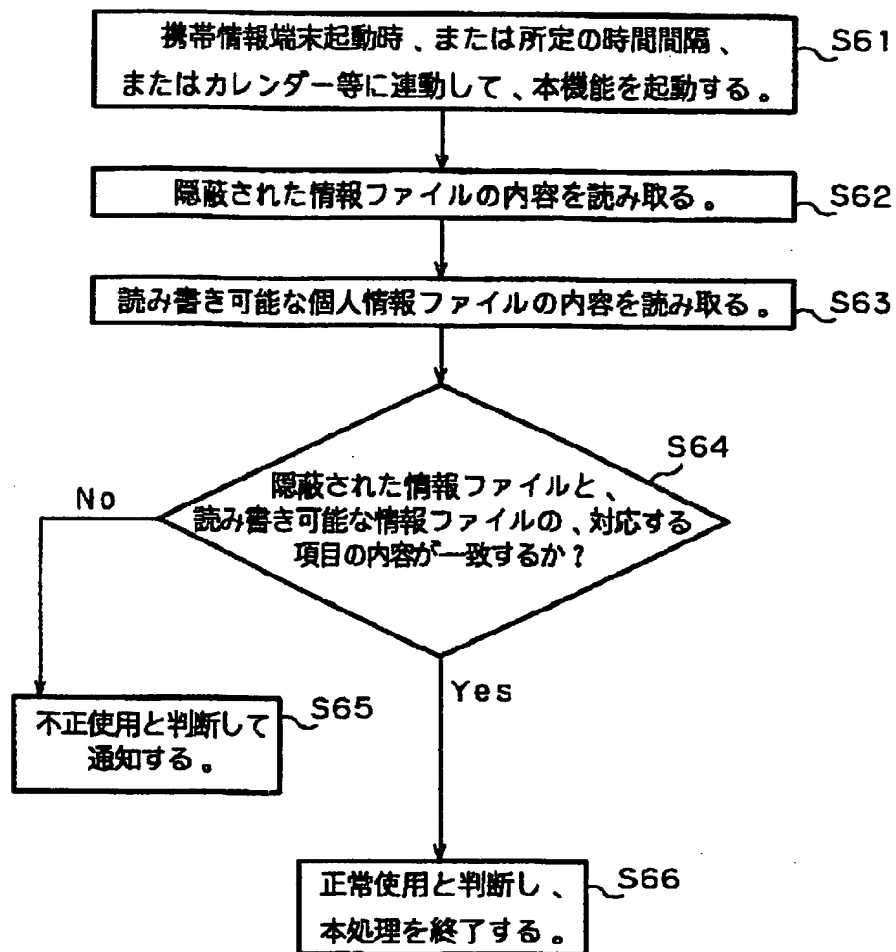
【図4】



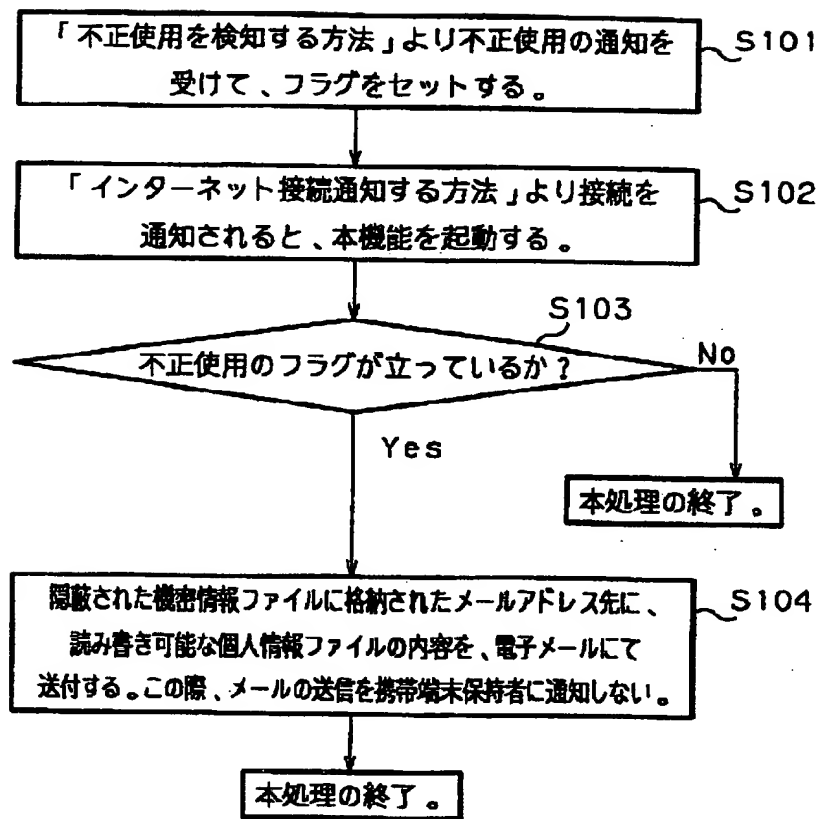
【図5】



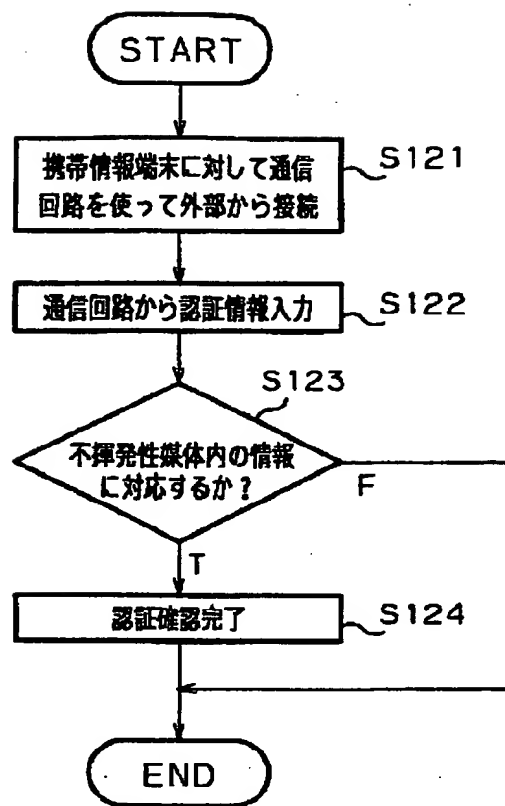
【図6】



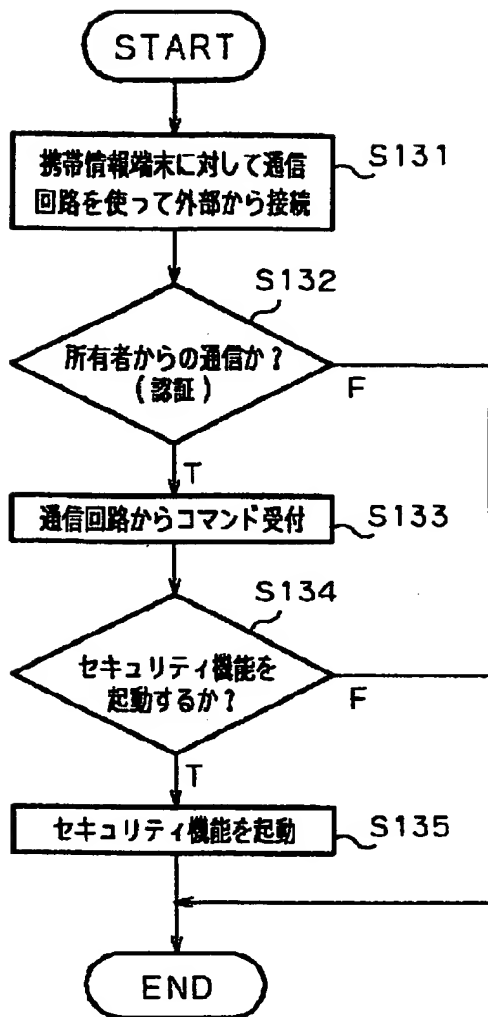
【図10】



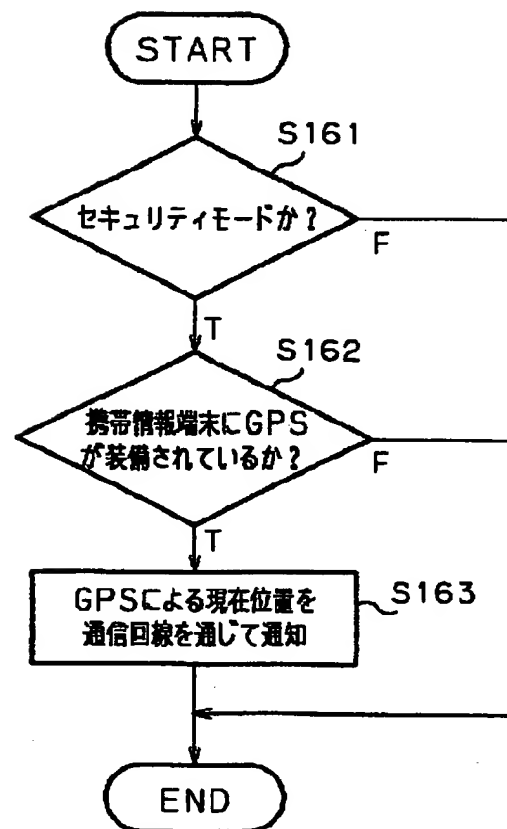
【図12】



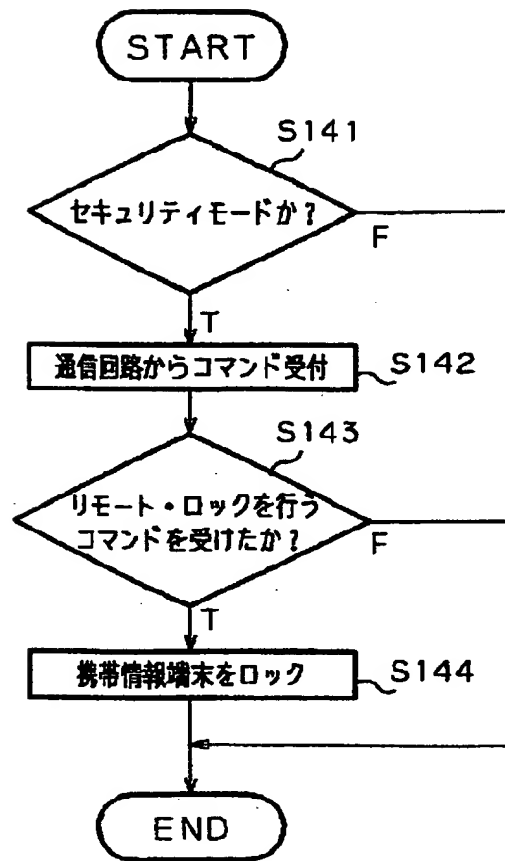
【図13】



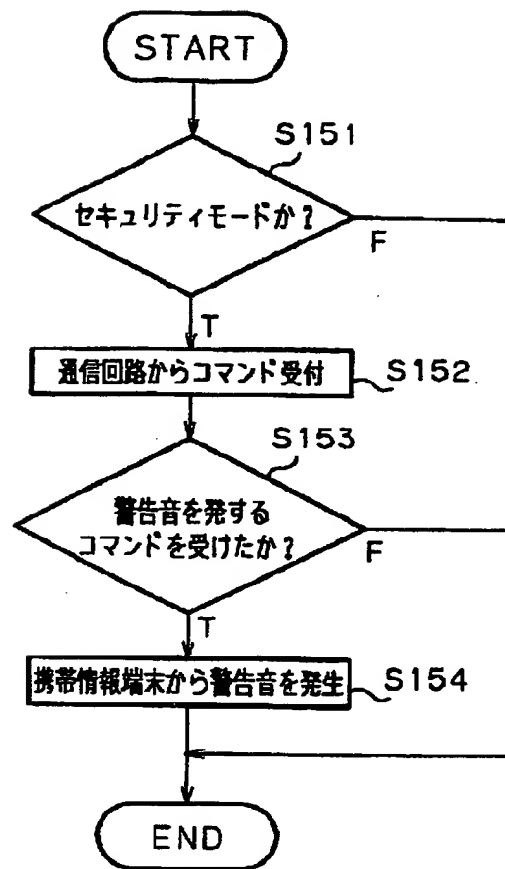
【図16】



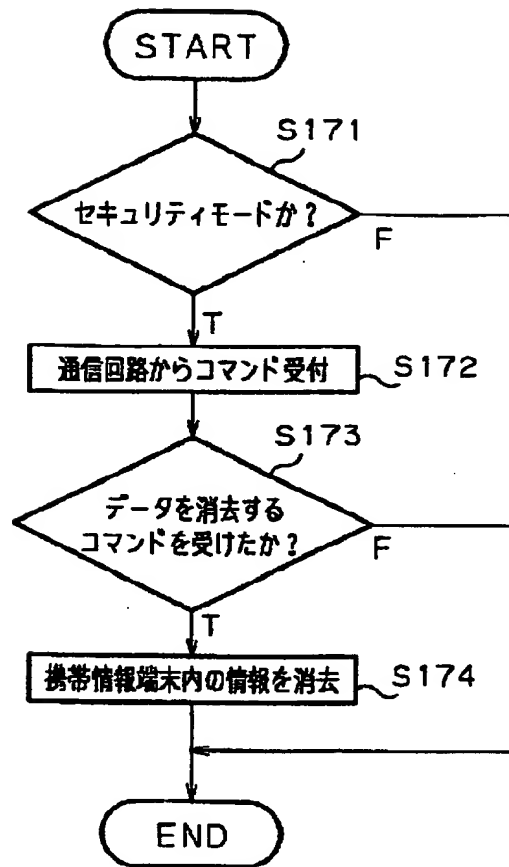
【図14】



【図15】



【図17】



【図18】

